Docket No.: 27592-01101-US1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Makoto Izawa et al.

Application No.: 10/710,987	Confirmation No.: 4986
Filed: August 16, 2004	Art Unit: 2437
For: Centralized Encryption Management System	Examiner: Shewaye Gelagay

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This brief is filed in furtherance of a Notice of Appeal filed on December 21, 2009 and upon receipt of a Notice of Panel Decision from Pre-Appeal Brief Review mailed on May 10, 2010. Applicants believe that any fees required in conjunction with this submission are indicated on an accompanying paper. However, should any further fees be due, including if such paper(s) be inadvertently omitted, Applicants authorize such fees to be charged to Deposit Account No. 22-0185, under Order No. 27592-01101-US1, from which the undersigned is authorized to draw.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206, which begin on the pages as indicated:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Onicix Group L.A., LLC

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 17 claims pending in this application.

B. Current Status of Claims

1. Claims canceled: 3
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1, 2, 4-18
4. Claims allowed: None
5. Claims rejected: 1, 2, 4-18

C. Claims On Appeal

The claims on appeal are Claims 1, 2, and 4-18.

IV. STATUS OF AMENDMENTS

Applicants did not file an Amendment After Final Rejection; all previous amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Briefly, various embodiments of the invention may relate to methods or systems for central management of encryption.

The application includes four independent claims. Independent Claim 1 is directed to a system, independent Claim 5 is directed to a system, independent Claim 14 is directed to a method, and independent Claim 18 is directed to a system.

Independent Claim 1 is directed to a system. The system of Claim 1 comprises an encryption apparatus configured to be connected between a plurality of communications terminals one or more having encrypting capability and the remainder having no encrypting capability, the encryption apparatus to perform an encrypting process or a decrypting process on data to enable encryption-based security between those of the plurality of communications terminals having encrypting capability and those of the plurality of communications terminals having no encrypting capability. The system of Claim 1 further comprises a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption. Additionally, the encryption apparatus further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process is performed. Exemplary embodiments that include these elements may be found, e.g., in Figs. 1, 2, 3, and/or 4 and in the specification at paragraphs 22-77.

To further explain one of the embodiments and its relationship to the claim elements, Fig. 1 shows one embodiment of such a system. In Fig. 1, blocks 1 are encryption apparatuses, and blocks 2-4 are various types of devices (terminals) without encryption capability. See, e.g., paragraphs [0022]-[0023]. Blocks 7-9 are various devices having encryption capability. See, e.g., paragraphs [0025]-[0026]. Hence, blocks 1 may correspond to "encryption apparatus configured to be connected between a plurality of communications terminals one or more having encrypting capability and the remainder having no encrypting capability." Blocks 1 are able to "perform an encrypting process or a decrypting process on data to enable encryption-based security between those of the plurality of communications terminals having encrypting capability and those of the plurality of communications terminals having no encrypting capability," as described, e.g., at paragraphs [0030]-[0032]. Fig. 1 also shows block 12, which is described as being "a manager terminal 12 for setting various information for the encryption/decryption." Paragraph [0024]. Paragraph [0024] further states, "when the manager terminal 12 sets various information onto each of the encryption apparatus 1, the access point 6, and the desktop PC 7," which establishes that manager terminal 12 may be understood as corresponding to "a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability," as in Claim 1. Paragraphs [0035]-[0042] address setting of information by manager terminal 12. The information specified in the language of Claim 1, namely, "the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption," may be understood, e.g., as corresponding to what is discussed in paragraphs [0037] (i.e., "[i]nformation for instructing to discard data packets (In particular, this information instructs to discard data packets, when data packets to be communicated between predetermined terminals have been received.)") and [0039] (i.e., "[i]nformation for instructing time when data encryption is to be performed"); see, also, paragraph [0005]. Finally, manager terminal is described, in some embodiments, as follows:

> The encryption apparatus 1 of this embodiment is characterized in that the IP-Sec serves as a bridge which links the two ports 33 and 34. In this connection, the term "bridge" indicates a function of sending data just as it is (which has inputted therein via one of the ports and then on which the encrypting or decrypting process has been performed) to another port without performing any routing process. In more detail, in the example shown in FIG. 5 data is inputted via the first port 33, and then the decrypting process is performed on the inputted data at the IP-Sec. Then, without performing on the encrypted data any routing process at the IP layer, the encrypted data (just as it is) is sent to and outputted from the second port 34. (In other words, without passing the encrypted data to the IP

> layer, the data after the decryption, just as it is, is sent to and outputted from the second port 34.) This manner corresponds to the above-mentioned "bridge" process. Namely, in the encryption apparatus 1 according to the present embodiment, the IP layer and the TCP/UDP layer are not used in the data transmission between the DB server 3 and the PC 9, and the data transmission process is carried out in layers lower than the IP layer.

Paragraph [0087]; see, also, Fig. 5. This may be understood as corresponding to "the encryption apparatus further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process is performed," as recited in Claim 1.

Independent Claim 5 is also directed to a system. The system of Claim 5 comprises an encryption apparatus having a plurality of ports configured to be connected between a plurality of communications terminals one or more having encryption capabilities and the remainder of the plurality of communications terminals having no encryption capabilities, the encryption apparatus to perform an encrypting process or a decrypting process on data received at one of a plurality of ports after passing through a data link layer and a physical layer. The encryption apparatus is configured to output encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled. Finally, the system of Claim 5 also includes a manager terminal to input information, including at least information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for encryption, into the encryption apparatus and those of the plurality of communications terminals having encryption capabilities, thereby completing a setting of each of the apparatus and communications terminals having encryption capabilities for communicating encrypted data.

Claim 5 may be related to the embodiment used above in conjunction with Claim 1 in a similar fashion. In particular, the various terminals, the manager terminal, and the encryption apparatus may be similarly understood. "The encryption apparatus is configured to output encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled" may be understood, for example, in conjunction with Fig. 5 and paragraph [0087], quoted above (note that ports 33 and 34 of Fig. 5, may be understood as corresponding to at least some of the claimed "plurality of ports").

Claim 14 is directed to a method. In particular, the method of Claim 14 comprises receiving data in an encryption apparatus configured to be connected between a plurality of communications terminals one or more having encryption capabilities and the remainder of the plurality of communications terminals having no encryption capabilities. The method further includes performing, by the encryption apparatus, an encrypting process or a decrypting process on data to terminate encryption-based security between at least one of the plurality of communications terminals having the encrypting capability and at least one of the plurality of communications terminals having no encrypting capability. Claim 14 also includes bridging data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process. Finally, Claim 14 also recites that information including whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for the encryption are inputted from a manager terminal into each of the encryption apparatus and those of the plurality of communications terminals having the encrypting capability.

The disclosed embodiment used in conjunction with Claims 1 and 5 above may similarly be used in conjunction with Claim 14. As shown and described in the sections discussed above, an encryption apparatus (e.g., block 1) receives data and may be connected between terminals having encryption capability (e.g., 7-9) and terminals without encryption capability (e.g., 1-3). The encryption apparatus may perform encryption or decryption, again, as discussed above. The claimed "bridging" is shown and described, e.g., in Fig. 5 and paragraph [0087]. Finally, the claimed "information…inputted from a manager terminal" has also been discussed above.

Finally, independent Claim 18 is directed to a system. The system of Claim 18 comprises a plurality of encryption apparatuses configured to be connected between a plurality of communications terminals having no encrypting capability, each of the plurality of encryption apparatuses to perform an encrypting process or a decrypting process on data to terminate encryption-based security between the communications terminals. The system also includes a manager terminal for inputting information including an indication of whether or not data packets are to be discarded between specific communications terminals after the data packets have been received, and including a time period for encryption into each of the encryption apparatuses. In the system of Claim 18, each of the encryption apparatuses further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process.

Applicants believe that the above discussions with respect to Claims 1 and 5 provide relationships between a disclosed embodiment and the various elements of Claim 18, which are similar to those of Claims 1 and/or 5.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-2, 4-9 and 12-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,604,807 to Yamaguchi et al. (hereinafter "Yamaguchi et al.") in view of "Transparent Network Security Policy Enforcement," USENIX 2000 (hereinafter "Keromytis et al.") and in view of U.S. Patent No. 6,775,769 to Inada et al. (hereinafter "Inada et al.") and in view of U.S. Patent No. 6,415,031 to Colligan et al. (hereinafter "Colligan et al.").

Claims 10-11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yamaguchi et al., in view of Keromytis et al. and in view of Inada et al. and in view of Colligan et al., and in view of U.S. Patent No. 5,481,610 to Doiron et al. (hereinafter "Doiron et al.").

VII. ARGUMENTS

A. INDEPENDENT CLAIMS 1, 5, 14, AND 18 ALL CONTAIN ELEMENTS RELATING TO "AN INDICATION OF WHETHER OR NOT DATA PACKETS ARE TO BE DISCARDED" THAT ARE NOT DISCLOSED OR SUGGESTED BY THE COMBINATION OF CITED REFERENCES.

Applicants respectfully submit that independent Claims 1, 5, 14, and 18, from which all other claims depend, all contain elements that are not disclosed or suggested by the combination of cited references. For example, independent Claim 1 includes recitation of "a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, ***the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received*** and a time period for encryption." (Emphasis added) Independent Claim 5 includes recitation of "a manager terminal to input information, ***including at least information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received*** and a time period for encryption, into the encryption apparatus and those of the plurality of communications terminals having encryption capabilities, thereby completing a setting of each of the apparatus and communications terminals having encryption capabilities for communicating encrypted data." (Emphasis added) Independent Claim 14 includes recitation of "***information including whether or not data packets are to be discarded between specific communications terminals after the data packets have been received*** and a time period for the encryption are inputted from a manager terminal into each of the encryption apparatus and those of the plurality of communications terminals having the encrypting capability." (Emphasis added) Finally, independent Claim 18 includes recitation of "a manager terminal for inputting ***information including an indication of whether or not data packets are to be discarded between specific communications terminals after the data packets have been received***, and including a time period for encryption into each of the encryption apparatuses." (Emphasis added)

The final Office Action (mailed December 21, 2009; hereinafter, "the Office Action"), noting page 4, acknowledges that "[Yamaguchi et al. and Keromytis et al.] do not explicitly disclose information including whether or not data packets are to be discarded between specific terminals after the data packets have been received." However, the Office Action then alleges that "Inada [et al.] in analogous art, however, discloses information including whether or not data packets are to be discarded between specific terminals after the data packets have been received (col. 5, line 25 – col. 6, line 65; col. 15, line 25 – col. 16, line 56; col. 17, lines 24-63)." Applicants respectfully disagree.

The cited portions of Inada et al. at cols. 5-6 describe "the function block configuration of a cryptographic apparatus," shown in Fig. 1. Col. 5, lines 16-17. During an interview conducted on January 19, 2010, the Examiner further pointed to col. 5, lines 23-31, which describe terminal function block 1 of Fig. 1, and which includes the discussion of "a management packet for managing the repeater-type cryptographic apparatus." Col. 5, lines 27-28. The remainder of this part of the cited portion includes discussion of "plaintext output filter 25," "ciphertext output filter 23," and "home station output filter 24." The discussions describe how these filters will discard "discard information." However, there is no nexus between the "management packet" and any information regarding the discarding of information/packets, i.e., there is no showing or discussion in Inada et al. that establishes that such a "management packet" contains such information. Therefore, at least this portion of Inada et al. fails to teach that the cryptographic apparatus receives from a manager terminal "information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received," as claimed.

Moving to col. 15, line 25 – col. 16, line 56, this portion of Inada et al. also provides description of a "home station input filter 31" and a "plaintext input filter 32" (with reference to Fig. 11). Again, there is no indication that "information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received" is provided to these filters.

Finally, col. 17, lines 24-63 appear to merely provide a summary of what was previously presented in Inada et al. They, too, fail to indicate the provision of "information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received."

An Advisory Action mailed on February 23, 2010 (hereinafter, "the Advisory Action") presents an alleged counterargument, "The Examiner disagrees[.] Inada teaches a management packet for managing cryptographic apparatus, or the like[,] that has similar function to that of a general terminal of connected to a network having an IP connection function (col. 5, lines 26-30)[,] which is adequate to meet the claimed limitation." Applicants note that a *packet*, of any type, is not a *terminal*, as claimed.

The Advisory Action continues, "The Applicant further argued that Inada does not specifically point out whether "the management packet" is coming from a management terminal or not. Examiner would like to point out that it is implicit that 'a management packet' can only come from a management apparatus." Applicants respectfully disagree, noting that many networks include management functionality performed among peer systems. For example, Martin-Flatin and Znaty have said:

> All DNM [(Distributed Network Management)] technologies, regardless of their idiosynchrasies, can be classified in two broad types: weakly and strongly distributed technologies, which implement respectively weakly and strongly distributed paradigms....*Strongly distributed paradigms*, on the other hand, decentralize management processing down to each and every agent: management tasks are no longer confined to NMSs [(Network Management Systems)], all agents and NMSs take part in the network management processing.

J.-P. Martin-Flatin and S. Znaty, "A Simple Typology of Distributed Network Management Paradigms," *the 8th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM'97)*, pp. 13-24, 30 July 1997. Hence, one cannot say that the presence of a "management packet" implicitly indicates a "manager terminal," as claimed, given that network management may be strongly distributed and, therefore, performed, e.g., in a cooperative fashion among the various terminals of the network.

The Advisory Action further states, "The ciphertext port 21 is an internal logical port positioned on the side of a ciphertext network for transferring ciphertext data received from the [ciphertext] network to the plaintext port 20 and the home station port 22, [and outputting data transferred from the plaintext port 20 or the home station port 22, here,] a packet to a ciphertext output filter 23." Applicants note that this was taken from Inada et al. at col. 5, lines 45-51, and Applicants have added some of the additional text from that section for clarity. The Advisory Action then states, "The ciphertext output filter 23 is a filter for a packet transferred to the ciphertext port 21 for determining the packet to be [a] discard packet which need not be transmitted from the ciphertext port 21, a transparent relay [packet not processed and transparently relayed] to the ciphertext network, or a ciphertext packet which needs to undergo encryption processing and discarding the packet if the packet is a discard packet." Applicants note that this is taken from Inada et al. at col. 5, lines 60-67, and that they have, again, added additional portions of the text of that section of Inada et al. to improve clarity. The Advisory Action then proceeds to cite Inada et al. at col. 8, lines 37-47, paraphrasing it as, "Inada further teaches a packet transferred to home station if it is a management packet containing information for managing the operation of the home station or the like and is sent to the terminal function block." The Advisory Action continues, "A management packet for managing can be processed. Thus the operation of the cryptographic apparatus can be managed as another machine changes setting of cryptographic processing of the cryptographic apparatus."

Applicants have reviewed this discussion from the Advisory Action and fail to see how this explains or proves that Inada et al. teaches or suggests the claim element for which it is allegedly being used. Even if, *arguendo*, Inada et al. did teach or suggest the claimed "management terminal," and even if the "management packet" of Inada et al. were sent by the management terminal (and Applicants respectfully disagree with this, as previously stated), the cited portions of Inada et al. fail to establish that the "management packet" contains "information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received."

The Office Action and the Advisory Action also fail to point out teachings from the other cited references that would address these shortcomings, and Applicants have not found such teachings.

It is, for at least these reasons, respectfully submitted that Claims 1, 5, 14, and 18, as well as their respective dependent claims, are allowable over the cited references (with respect to the dependent claims rejected based on Doiron et al., Applicants respectfully submit that this further reference also fails to cure the deficiencies discussed above).

B. INDEPENDENT CLAIMS 1, 5, 14, AND 18 ALL CONTAIN ELEMENTS RELATING TO "A TIME PERIOD FOR ENCRYPTION" THAT ARE NOT DISCLOSED OR SUGGESTED BY THE COMBINATION OF CITED REFERENCES.

Applicants respectfully submit that independent Claims 1, 5, 14, and 18, from which all other claims depend, all contain elements that are not disclosed or suggested by the combination of cited references. For example, independent Claim 1 includes recitation of "a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and ***a time period for encryption***." (Emphasis added) Independent Claim 5 includes recitation of "a manager terminal to input information, including at least information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and ***a time period for encryption***, into the encryption apparatus and those of the plurality of communications terminals having encryption capabilities, thereby completing a setting of each of the apparatus and communications terminals having encryption capabilities for communicating encrypted data." (Emphasis added) Independent Claim 14 includes recitation of "information including whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and ***a time period for the encryption*** are inputted from a manager terminal into each of the encryption apparatus and those of the plurality of communications terminals having the encrypting capability." (Emphasis added) Finally, independent Claim 18 includes recitation of "a manager terminal for inputting information including an indication of whether or not data packets are to be discarded between specific communications terminals after the data packets have been received, ***and including a time period for encryption*** into each of the encryption apparatuses." (Emphasis added)

The Office Action, noting page 5, further states, "None of the references explicitly disclose input information including a time period for encryption." Applicants agree with this assessment of the references. The Office Action then alleges, "Colligan [et al.] in analogous art, however, discloses inputting information including a time period for encryption. (col. 8, line 7-18; col. 8, line 65 – col. 9, line 5)." Applicants respectfully disagree.

Applicants note that the cited portions of Colligan et al., at cols. 8-9, refer to the encryption of information in a video-on-demand (VOD) source 402 (see, e.g., col. 7, lines 60 ff.) and discuss scheduling of encryption and the use of an encryption key based on "an appropriate time epoch." Col. 9, lines 25-26. Applicants also note the discussion of cols. 5-7 of Colligan et al., during the above-summarized interview. These portions of Colligan et al. refer to the furnishing of encrypted information to a remote server 404 and how it may be decrypted and then re-encrypted at the video server. However, nowhere is there any discussion of providing "a time period for encryption," as claimed, to the server. On the contrary, Colligan et al. discusses, e.g., at col. 5, lines 29-37, "Subsequently, when the remote server (404) receives (508) a request for transmission of the video program from a subscriber station (110), the remote server (404) responds by first decrypting (510) the video program from the first encrypted form. A first key is may be [sic] used to accomplish such decryption (510), and such key may have been received from the video on-demand source (402) via a communication channel that is separate from the one used to transmit the video program." See, also, col. 6, lines 13-24 and lines 57-64, and col. 7, lines 13-19. In all of these cases, there is no time period information transmitted to the server (or to any other component) in Inada et al.; on the contrary, the key necessary for decryption is provided, and therefore, there is no need to provide such "a time period for encryption."

The Advisory Action attempts to provide counterarguments. As noted above, the Advisory Action initially attempts to establish that there is a "management terminal" implicit in Inada et al. Applicants respectfully disagree with this for at least the reasons noted above.

Following the discussion related to the "information for instruction whether or not data packets are to be discarded," treated above, the Advisory Action continues, in an attempt to rebut Applicants' arguments regarding the providing of "a time period for encryption." In particular, the Advisory Action states the following:

> Applicant argued that "Colligan does not teach inputting a time period for encryption." The Examiner would like to point out that Colligan teaches "an encryption coordinator receives the content and schedules the content for encryption and distributed to a set of Remote servers. [*sic*] The encryptor uses the particular key corresponding to the first time to decrypt the content and uses a particular key corresponding to a second time to re-encrypt the content... The remote server re-encrypts the video program into a second encrypted [*sic*] from using a second key." The Examiner would like to point out that since the encryption is performed according to a schedule and reencrypted and distributed by the distribution server to the subscriber station, the decryption process has to also be performed according [to the] schedule using a particular key corresponding to a first time or a second time.

Advisory Action at 2.

Applicants emphasize that what is recited, e.g., in Claim 1 includes, "***a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including*** an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and ***a time period for encryption***." Hence, even if, *arguendo*, one looks to Colligan et al. for a teaching that encryption may have an associated time period, and Applicants are unclear, based on the above, as to how the Advisory Action is relying on Colligan et al. in this particular discussion, this fails to teach or suggest what is claimed, e.g., in Claim 1, namely, "a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including...a time period for encryption." (Applicants note the similar elements cited above in the other independent claims, although the other independent claims are of varying scopes.) As noted above, Colligan et al. altogether fails to address the transmission of time-related information (and does not need to do so, for the reasons discussed above).

Applicants have also reviewed the other cited references and have found no teachings or suggestions that would cure these deficiencies of Colligan et al.

It is, for at least these further reasons, respectfully submitted that Claims 1, 5, 14, and 18, as well as their respective dependent claims, are allowable over the cited references (with respect to the dependent claims rejected based on Dairon et al., Applicants respectfully submit that this further reference fails to cure the deficiencies of the other cited references).

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS

No related proceedings are referenced in II. above, so no Appendix is included.

Dated: June 2, 2010

Respectfully submitted,

By
Jeffrey W. Gluck, Ph.D.
Registration No.: 44,457
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, N.W., Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 572-0322 (Direct Dial)
(202) 293-6229 (Fax)
Attorney for Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 10/710,987:

1. A system, comprising:

an encryption apparatus configured to be connected between a plurality of communications terminals one or more having encrypting capability and the remainder having no encrypting capability, the encryption apparatus to perform an encrypting process or a decrypting process on data to enable encryption-based security between those of the plurality of communications terminals having encrypting capability and those of the plurality of communications terminals having no encrypting capability; and

a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption;

wherein the encryption apparatus further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process is performed.

2. The system according to claim 1, wherein the encryption apparatus is configured to receive data from and retransmit the data in the form of encrypted data to one of the plurality of communications terminals having encrypting capability, and the encryption apparatus is configured to receive and retransmit the data in the form of non-encrypted data from and to one of the plurality of communications terminals having no encrypting capability.

4. The system according to claim 1, wherein:

the encryption apparatus further includes a storage to store the information inputted from the manager terminal; and wherein the encryption apparatus in performing the encrypting process and the decrypting process by is configured to compare the information stored in the storage with header information of a data packet of data received through one of the plurality of ports.

5. A system, comprising:

an encryption apparatus having a plurality of ports configured to be connected between a plurality of communications terminals one or more having encryption capabilities and the remainder of the plurality of communications terminals having no encryption capabilities, the encryption apparatus to perform an encrypting process or a decrypting process on data received at one of a plurality of ports after passing through a data link layer and a physical layer,

wherein the encryption apparatus is configured to output encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled; and

a manager terminal to input information, including at least information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for encryption, into the encryption apparatus and those of the plurality of communications terminals having encryption capabilities, thereby completing a setting of each of the apparatus and communications terminals having encryption capabilities for communicating encrypted data.

6. The system according to claim 5, wherein:

the encryption apparatus further includes a storage to store the information inputted from the manager terminal; and wherein

the encryption apparatus, in performing the encrypting process and the decrypting process is configured to compare the information stored in the storage with header information of a data packet of data received through one of the plurality of ports.

7. The system according to claim 1, wherein the information comprises at least one of information associated with the presence or absence of encryption or decryption process, the

availability of packet communications, an encryption level, a time period to perform encryption, an encryption policy, or an encryption key.

8. The system according to claim 1, wherein the plurality of communications terminals are inside a secured network.

9. The system according to claim 1, wherein at least one of the plurality of communications terminals is outside a secured network.

10. The system according to claim 1, wherein the encryption apparatus comprises a data path for a connected terminal and wherein the encryption apparatus is configured to perform the encryption process or the decryption process on data received or transmitted on each data path using a different encryption key associated with the connected terminal.

11. The system according to claim 1, wherein the those of plurality of communications terminals having encrypting capability are connected to the encryption apparatus through an access point.

12. The system according to claim 1, wherein the plurality of communications terminals are arranged in a plurality of local area networks.

13. The system according to claim 12, comprising a plurality of manager terminals, each of the plurality of manager terminals to manage encryption and decryption settings in at least one communications terminal having the encrypting capabilities in at least one of the plurality of local area networks.

14. A method, comprising:

receiving data in an encryption apparatus configured to be connected between a plurality of communications terminals one or more having encryption capabilities and the remainder of the plurality of communications terminals having no encryption capabilities;

performing, by the encryption apparatus, an encrypting process or a decrypting process on data to terminate encryption-based security between at least one of the plurality of communications terminals having the encrypting capability and at least one of the plurality of communications terminals having no encrypting capability; and

bridging data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process, wherein

information including whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for the encryption are inputted from a manager terminal into each of the encryption apparatus and those of the plurality of communications terminals having the encrypting capability.

15. The method according to claim 14, comprising:

receiving and retransmitting, by the encryption apparatus, encrypted data from and to one of the plurality of communications terminals having the encrypting capability; and

receiving and retransmitting, by the encryption apparatus, non-encrypted data from and to one of the plurality of communications terminals having no encrypting capability.

16. The method according to claim 14, comprising:

storing, by the encryption apparatus, information inputted from a manager terminal; and

controlling the encrypting process and the decrypting process by comparing the information stored in a storage with header information of a data packet of the data received through one of the plurality of ports.

17. The method according to claim 14, comprising:

performing an encrypting process or a decrypting process on data received at one of the plurality of ports after passing through a data link layer and a physical layer; and

outputting encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled.

18. A system, comprising:

a plurality of encryption apparatuses configured to be connected between a plurality of communications terminals having no encrypting capability, each of the plurality of encryption apparatuses to perform an encrypting process or a decrypting process on data to terminate encryption-based security between the communications terminals; and

a manager terminal for inputting information including an indication of whether or not data packets are to be discarded between specific communications terminals after the data packets have been received, and including a time period for encryption into each of the encryption apparatuses;

wherein each of the encryption apparatuses further include a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process.